

FMCとFTDのスマートライセンス登録と一般的な問題を使用したトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[FMCスマートライセンスの登録](#)

[前提条件](#)

[FMCスマートライセンスの登録](#)

[Smart Software Manager\(SSM\)側での確認](#)

[FMCスマートライセンスの登録解除](#)

[RMA](#)

[トラブルシューティング](#)

[一般的な問題](#)

[ケーススタディ 1無効トークン](#)

[ケーススタディ 2無効なDNS](#)

[ケーススタディ 3無効な時間値](#)

[ケーススタディ 4サブスクリプションなし](#)

[ケーススタディ 5コンプライアンス違反\(OOC\)](#)

[ケーススタディ 6強力な暗号化なし](#)

[追加情報](#)

[スマートライセンスの状態の通知の設定](#)

[FMCからのヘルスアラート通知の取得](#)

[同じスマートアカウントの複数のFMC](#)

[FMCがインターネット接続を維持する必要がある](#)

[複数のFMCvの導入](#)

[FAQ](#)

[関連情報](#)

はじめに

このドキュメントでは、Firepower Threat Defense(FTD)管理対象デバイス上のFirepower Management Centerのスマートライセンス登録の設定について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

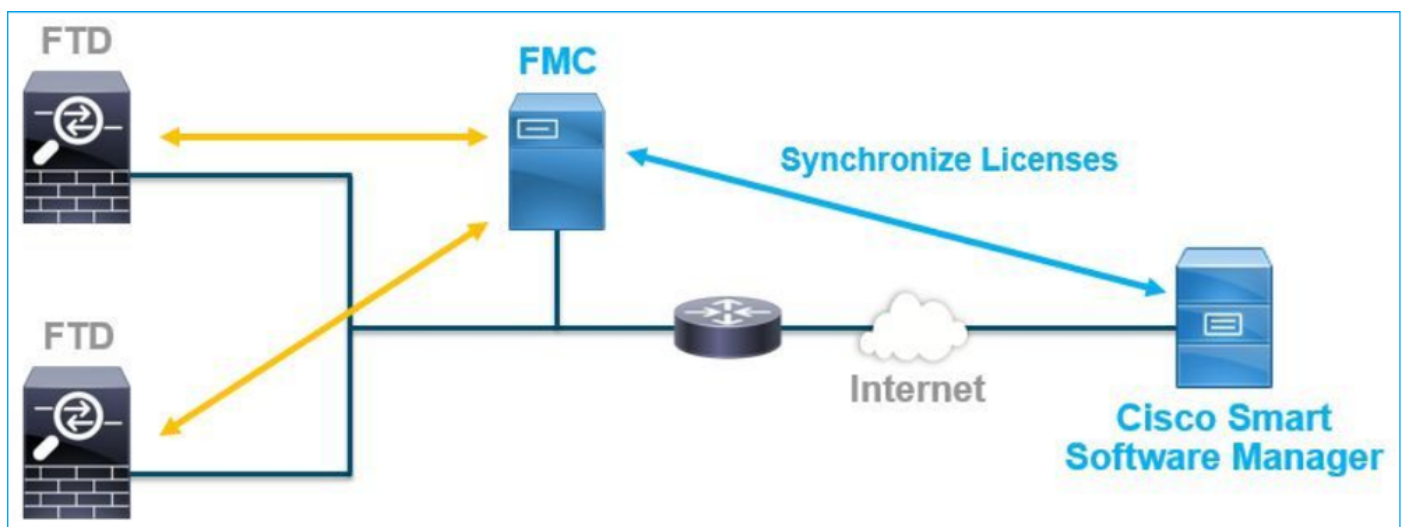
使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

FMC、FTD、およびスマートライセンスの登録

スマートライセンスの登録は、Firepower Management Center(FMC)で実行されます。FMCは、インターネット経由でCisco Smart Software Manager(CSSM)ポータルと通信します。CSSMでは、ファイアウォール管理者がスマートアカウントとそのライセンスを管理します。FMCは、管理対象のFirepower脅威対策(FTD)デバイスに対してライセンスを自由に割り当てたり、削除したりできます。つまり、FTDデバイスのライセンスはFMCによって一元管理されます。



FTDデバイスの特定の機能を使用するには、追加ライセンスが必要です。お客様がFTDデバイスに割り当てることができるスマートライセンスタイプについては、「[FTDのライセンスタイプと制限事項](#)」を参照してください。

BaseライセンスはFTDデバイスに含まれています。このライセンスは、FMCがCSSMに登録されると、スマートアカウントに自動的に登録されます。

期間ベースのライセンス：脅威、マルウェア、およびURLフィルタリングはオプションです。ライセンスに関連する機能を使用するには、ライセンスをFTDデバイスに割り当てる必要があります。

FTDの管理にFirepower Management Center Virtual(FMCv)を使用するには、FMCvに対してCSSMのFirepowerMCvデバイスライセンスも必要です。

FMCvライセンスはソフトウェアに含まれており、永続的です。

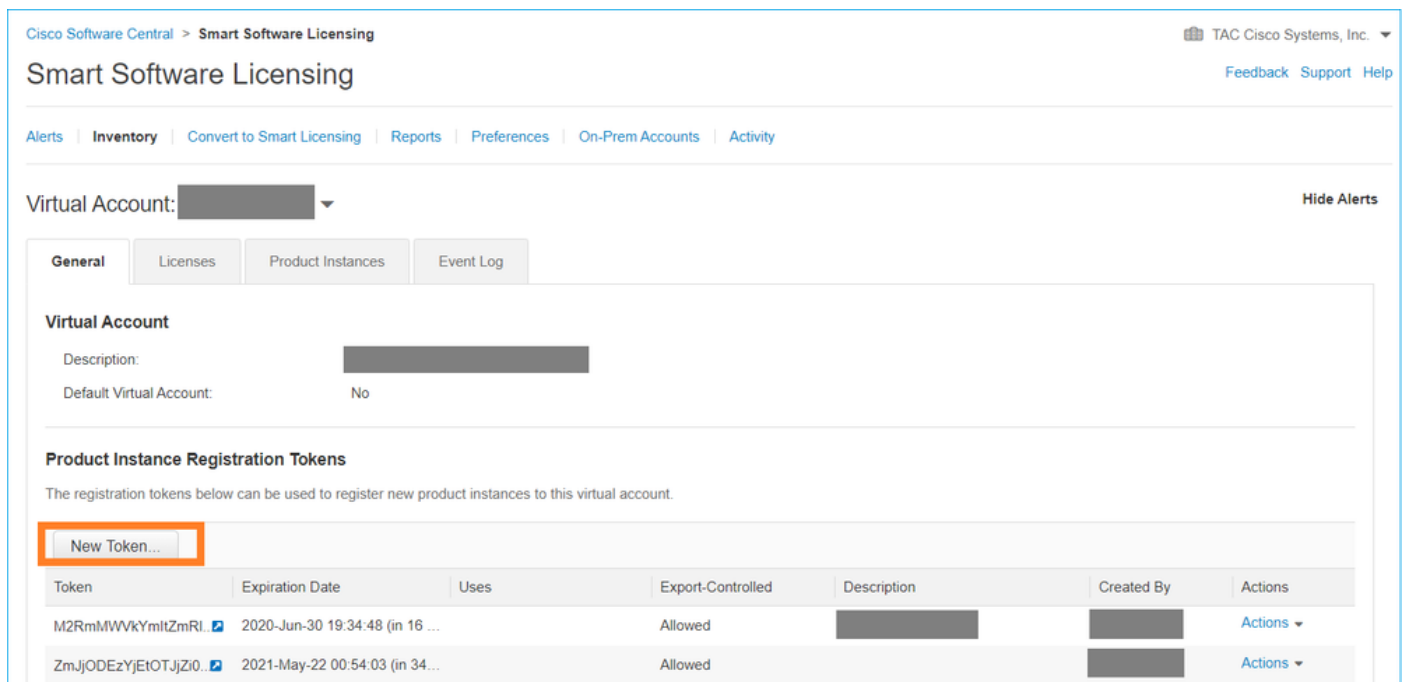
また、発生する可能性のある一般的なライセンス登録エラーのトラブルシューティングに役立つシナリオが、このドキュメントに記載されています。

ライセンスの詳細については、『[シスコFirepowerシステム機能ライセンス](#)』および『[Firepowerライセンスに関するよくある質問\(FAQ\)](#)』を参照してください。

FMCスマートライセンスの登録

前提条件

1. スマートライセンス登録を行うには、FMCがインターネットにアクセスする必要があります。証明書はFMCとスマートライセンスクラウドの間でHTTPSを使用して交換されるため、通信に影響を与えたり、通信を変更したりする可能性のあるデバイスがパス上にないことを確認します。(ファイアウォール、プロキシ、SSL復号化デバイスなど)。
2. CSSMにアクセスし、次の図に示すようにInventory > General > New TokenボタンからトークンIDを発行します。



The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The breadcrumb navigation is 'Cisco Software Central > Smart Software Licensing'. The page title is 'Smart Software Licensing' with links for 'Feedback', 'Support', and 'Help'. A navigation bar includes 'Alerts', 'Inventory', 'Convert to Smart Licensing', 'Reports', 'Preferences', 'On-Prem Accounts', and 'Activity'. A 'Virtual Account' dropdown is set to a redacted value, and there is a 'Hide Alerts' link. The 'General' tab is selected, showing 'Virtual Account' details (Description: redacted, Default Virtual Account: No) and 'Product Instance Registration Tokens'. A table lists two tokens with columns for Token, Expiration Date, Uses, Export-Controlled, Description, Created By, and Actions. The 'New Token...' button is highlighted with an orange box.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
M2RmMwVkyMitZmRI. [lock]	2020-Jun-30 19:34:48 (in 16 ...)		Allowed	[redacted]	[redacted]	Actions ▾
ZmJjODEzYjEtOTJjZi0. [lock]	2021-May-22 00:54:03 (in 34 ...)		Allowed		[redacted]	Actions ▾

強力な暗号化を使用するには、Allow export-controlled functionality on the products registered with this tokenオプションを有効にします。有効にすると、チェックボックスにチェックマークが表示されます。

3. Create Tokenを選択します。

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:

* Expire After: Days
Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

Allow export-controlled functionality on the products registered with this token ?

[Create Token](#) [Cancel](#)

FMCスマートライセンスの登録

次の図に示すように、FMCでSystem> Licenses > Smart Licensesの順に移動し、Registerボタンを選択します。

Firepower Management Center
 System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects AMP Intelligence

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register

[Register](#)

Smart License Status

Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--
Cisco Success Network:	--
Cisco Support Diagnostics:	--

次の図に示すように、Smart Licensing Product RegistrationウィンドウでトークンIDを入力し、Apply Changesを選択します。

Smart Licensing Product Registration

Product Instance Registration Token:

OWI4Mzc5MTAtNzQwYi00YTVILTkyNTktMGMxNGJlYmRmNDUwLTE1OTQ3OTQ5%
0ANzc3ODB8SnVXc2tPaks4SE5Jc25xTDkySnFYempTZnJEWVdVQU1SU1NiOWFM

If you do not have your ID token, you may copy it from your Smart Software manager The under the assigned virtual account. [Cisco Smart Software Manager](#)

Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.

Cisco Success Network

The Cisco Success Network provides usage information and statistics to Cisco. This information allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [sample data](#) that will be sent to Cisco.

Enable Cisco Success Network

Cisco Support Diagnostics

The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration and operational health data from your devices and process that data through our automated problem detection system, and proactively notify you of issues detected. To view a sample

Internet connection is required.

Cancel

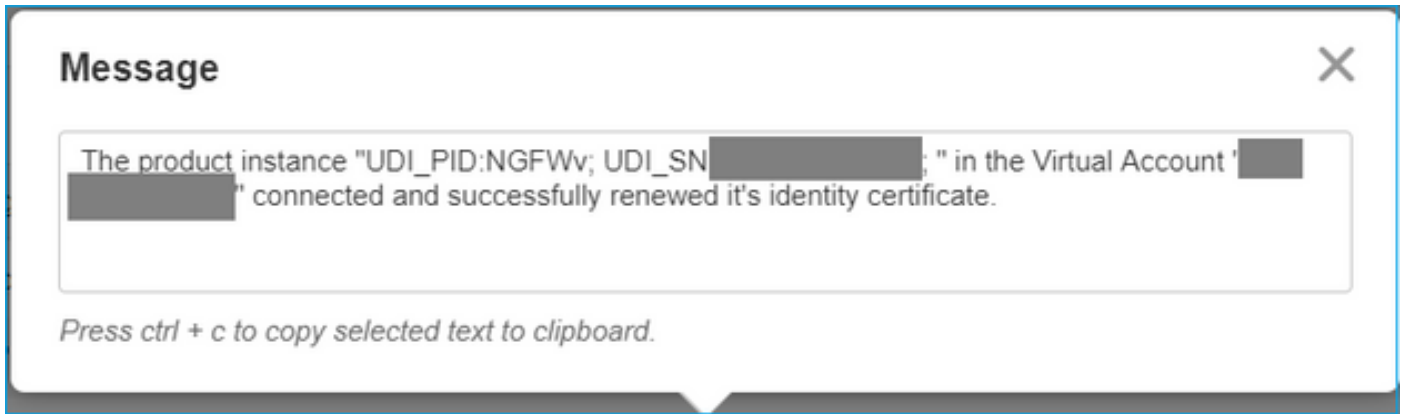
Apply Changes

スマートライセンスが正常に登録されると、次の図に示すように、製品登録のステータスが Registered と表示されます。

FTDデバイスに期間ベースライセンスを割り当てるには、Edit Licensesを選択します。次に、管理対象デバイスを選択して、ライセンスを持つデバイスのセクションに追加します。最後に、次の図に示すようにApplyボタンを選択します。

Smart Software Manager(SSM)側での確認

FMCスマートライセンスの登録が正常に行われたことは、次の図に示すように、CSSMのInventory > Event Logで確認できます。

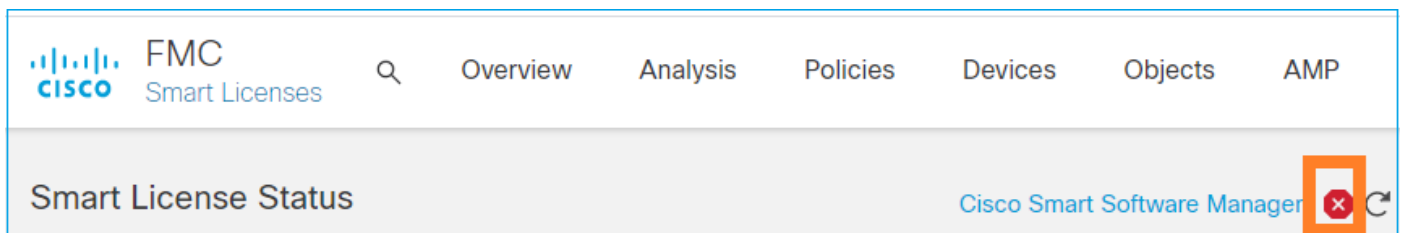


FMCの登録ステータスは、Inventory > Product Instancesで確認できます。Event Logタブでイベントログを確認します。スマートライセンスの登録と使用状況は、Inventory > Licensesタブで確認できます。購入した期間ベースのライセンスが正しく使用され、ライセンス不足を示すアラートがないことを確認します。

FMCスマートライセンスの登録解除

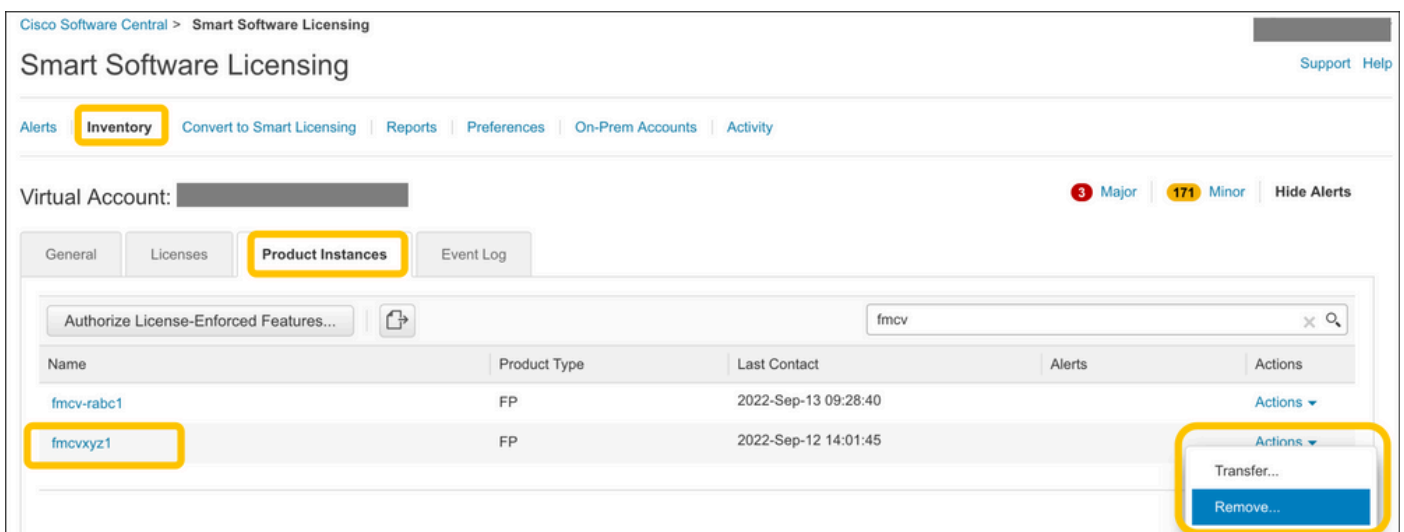
Cisco SSMからのFMCの登録解除

何らかの理由でライセンスをリリースするか、別のトークンを使用するには、次の図に示すように、System > Licenses > Smart Licensesの順に移動し、登録解除ボタンを選択します。



SSM側からの登録の削除

Smart Software Manager([Cisco Smart Software Manager](#))にアクセスし、[Inventory > Product Instances](#)の順に選択して、ターゲットFMCで[Remove](#)を選択します。次に、Remove Product Instanceを選択してFMCを削除し、割り当てられたライセンスを解放します(次の図を参照)。





Confirm Remove Product Instance

If you continue, the product instance "fmcvxyz1" will no longer appear in the Smart Software Manager and will no longer be consuming any licenses. In order to bring it back, you will need to re-register the product instance.

Remove Product Instance

Cancel

RMA

FMCがRMAを受けた場合は、「FMCスマートライセンスの登録解除> SSM側からの登録の削除」セクションの手順を使用してCisco Smart Software Manager(CSSM)からFMCを登録解除してから、「FMCスマートライセンスの登録」セクションの手順を使用してCSSMにFMCを再登録します。

トラブルシューティング

時刻同期検証

FMC CLI (SSHなど) にアクセスし、時刻が正しく、信頼できるNTPサーバと同期されていることを確認します。証明書はスマートライセンス認証に使用されるため、FMCに正しい時刻情報が含まれていることが重要です。

```
<#root>
```

```
admin@FMC:~$
```

```
date  
Thu
```

```
Jun 14 09:18:47 UTC 2020  
admin@FMC:~$  
admin@FMC:~$
```

```
ntpq -pn
```


remote	refid	st	t	when	poll	reach	delay	offset	jitter
*10.0.0.2	171.68.xx.xx	2	u	387	1024	377	0.977	0.469	0.916
127.127.1.1	.SFCL.	13	l	-	64	0	0.000	0.000	0.000

FMCのUIで、System > Configuration > Time Synchronizationの順に選択して、NTPサーバの値を確認します。

名前解決を有効にして、tools.cisco.comへの到達可能性を確認する

FMCがFQDNを解決でき、tools.cisco.comに到達できることを確認します。

```
<#root>
```

```
>
```

```
expert
admin@FMC2000-2:~$
```

```
sudo su
```

```
Password:
root@FMC2000-2:/Volume/home/admin# ping tools.cisco.com
PING tools.cisco.com (173.37.145.8) 56(84) bytes of data:
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=1 ttl=237 time=163 ms
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=2 ttl=237 time=163 ms
```

FMCのUIで、System > Configuration > Management Interfacesから管理IPとDNSサーバのIPを確認します。

FMCからtools.cisco.comへのHTTPS(TCP 443)アクセスの確認

Telnetまたはcurlコマンドを使用して、FMCがtools.cisco.comにHTTPSアクセスできることを確認します。TCP 443通信が切断されている場合は、ファイアウォールによってブロックされていないこと、およびパスにSSL復号化デバイスがないことを確認します。

```
<#root>
```

```
root@FMC2000-2:/Volume/home/admin#
telnet tools.cisco.com 443
Trying 72.163.4.38...
Connected to tools.cisco.com.
Escape character is '^]'.
^CConnection closed by foreign host.
<--- Press Ctrl+C
```

カールテスト :

<#root>

```
root@FMC2000-2:/Volume/home/admin#
```

```
curl -vvk https://tools.cisco.com
```

```
*
```

```
Trying 72.163.4.38...
```

```
* TCP_NODELAY set
```

```
* Connected to tools.cisco.com (72.163.4.38) port 443 (#0)
```

```
* ALPN, offering http/1.1
```

```
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
```

```
* successfully set certificate verify locations:
```

```
* CAfile: /etc/ssl/certs/ca-certificates.crt
```

```
CApath: none
```

```
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
```

```
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
```

```
* TLSv1.2 (IN), TLS handshake, Server hello (2):
```

```
* TLSv1.2 (IN), TLS handshake, Certificate (11):
```

```
* TLSv1.2 (IN), TLS handshake, Server finished (14):
```

```
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
```

```
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
```

```
* TLSv1.2 (OUT), TLS handshake, Finished (20):
```

```
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
```

```
* TLSv1.2 (IN), TLS handshake, Finished (20):
```

```
* SSL connection using TLSv1.2 / AES128-GCM-SHA256
```

```
* ALPN, server accepted to use http/1.1
```

```
* Server certificate:
```

```
* subject: C=US; ST=CA; L=San Jose; O=Cisco Systems, Inc.; CN=tools.cisco.com
```

```
* start date: Sep 17 04:00:58 2018 GMT
```

```
* expire date: Sep 17 04:10:00 2020 GMT
```

```
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
```

```
* SSL certificate verify ok.
```

```
> GET / HTTP/1.1
```

```
> Host: tools.cisco.com
```

```
> User-Agent: curl/7.62.0
```

```
> Accept: */*
```

```
>
```

```
< HTTP/1.1 200 OK
```

```
< Date: Wed, 17 Jun 2020 10:28:31 GMT
```

```
< Last-Modified: Thu, 20 Dec 2012 23:46:09 GMT
```

```
< ETag: "39b01e46-151-4d15155dd459d"
```

```
< Accept-Ranges: bytes
```

```
< Content-Length: 337
```

```
< Access-Control-Allow-Credentials: true
```

```
< Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
```

```
< Access-Control-Allow-Headers: Content-type, fromPartyID, inputFormat, outputFormat, Authorization, Co
```

```
< Content-Type: text/html
```

```
< Set-Cookie: CP_GUTC=10.163.4.54.1592389711389899; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain
```

```
< Set-Cookie: CP_GUTC=10.163.44.92.1592389711391532; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain
```

```
< Cache-Control: max-age=0
```

```
< Expires: Wed, 17 Jun 2020 10:28:31 GMT
```

```
<
```

```
<html>
```

```
<head>
```

```
<script language="JavaScript">
```

```
var input = document.URL.indexOf('intellishield');
if(input != -1) {
  window.location="https://intellishield.cisco.com/security/alertmanager/";
}
else {
  window.location="http://www.cisco.com";
};

</script>
</head>

<body>
<a href="http://www.cisco.com">www.cisco.com</a>
</body>
</html>
* Connection #0 to host tools.cisco.com left intact
root@FMC2000-2:/Volume/home/admin#
```

DNSの検証

tools.cisco.comへの解決が正常に完了したことを確認します。

```
<#root>

root@FMC2000-2:/Volume/home/admin#

nslookup tools.cisco.com

Server:          192.0.2.100
Address:         192.0.2.100#53

Non-authoritative answer:

Name:   tools.cisco.com
Address: 72.163.4.38
```

プロキシの検証

apProxyを使用する場合は、FMCとプロキシサーバ側の両方の値を確認します。FMCで、FMCが正しいプロキシサーバIPとポートを使用しているかどうかを確認します。

```
<#root>

root@FMC2000-2:/Volume/home/admin#

cat /etc/sf/smart_callhome.conf

KEEP_SYNC_ACTIVE:1
PROXY_DST_URL:https://tools.cisco.com/its/service/oddce/services/DDCEService

PROXY_SRV:192.0.xx.xx

PROXY_PORT:80
```

FMCのUIでは、プロキシ値はSystem > Configuration > Management Interfacesで確認できます。

FMC側の値が正しい場合は、プロキシサーバ側の値を確認します(たとえば、プロキシサーバがFMCおよびtools.cisco.comへのアクセスを許可している場合)。さらに、プロキシを介したトラフィックと証明書交換を許可します。FMCは、スマートライセンス登録に証明書を使用します)。

期限切れトークンID

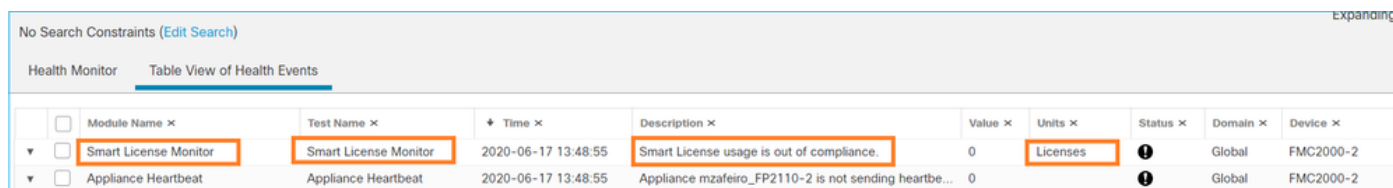
発行されたトークンIDが期限切れでないことを確認します。有効期限が切れている場合は、Smart Software Manager管理者に新しいトークンを発行し、新しいトークンIDでスマートライセンスを再登録するように依頼します。

FMCゲートウェイの変更

リレープロキシやSSL復号化デバイスの影響により、スマートライセンス認証を正しく実行できない場合があります。可能であれば、これらのデバイスを回避するようにFMCインターネットアクセスのルートを変更し、スマートライセンスの登録を再試行します。

FMCのヘルスイベントの確認

FMCで、System > Health > Eventsの順に移動し、Smart License Monitorモジュールのステータスにエラーがないかどうかを確認します。たとえば、証明書の期限切れが原因で接続が失敗すると、次の図に示すように、id certificated expiredなどのエラーが生成されます。



Module Name	Test Name	Time	Description	Value	Units	Status	Domain	Device
Smart License Monitor	Smart License Monitor	2020-06-17 13:48:55	Smart License usage is out of compliance.	0	Licenses	Warning	Global	FMC2000-2
Appliance Heartbeat	Appliance Heartbeat	2020-06-17 13:48:55	Appliance mzafeiro_FP2110-2 is not sending heartbe...	0		Warning	Global	FMC2000-2

SSM側のイベントログの確認

FMCがCSSMに接続できる場合は、Inventory > Event Logで接続のイベントログを確認します。CSSMにそのようなイベントログまたはエラーログがあるかどうかを確認します。FMCサイトの値/動作に問題がなく、CSSM側にイベントログがない場合は、FMCとCSSM間のルートに問題がある可能性があります。

一般的な問題

登録および許可の状態の概要：

製品登録状況	使用許可状態	注釈
未登録	—	FMCが登録モードでも評価モードでもない。これは、FMCのインストール後、または評価ライセンスの

		有効期限が90日後の初期状態です。
登録済み	承認済み	FMCはCisco Smart Software Manager(CSSM)に登録され、有効なサブスクリプションに登録されたFTDデバイスがあります。
登録済み	認証が期限切れ	FMCがシスコライセンスバックエンドと90日以上通信できませんでした。
登録済み	未登録	FMCはCisco Smart Software Manager(CSSM)に登録されていますが、FMCに登録されているFTDデバイスはありません。
登録済み	コンプライアンス違反	FMCはCisco Smart Software Manager(CSSM)に登録されていますが、無効なサブスクリプションに登録されているFTDデバイスがあります。 たとえば、FTD(FP4112)デバイスはTHREATサブスクリプションを使用しますが、Cisco Smart Software Manager(CSSM)を使用すると、FP4112で使用できるTHREATサブスクリプションはありません。
評価 (90日)	N/A	評価期間は使用中ですが、FMCに登録されているFTDデバイスはありません。

ケース スタディ 1無効トークン

症状：次の図に示すように、無効なトークンが原因でCSSMへの登録が急速に失敗します (~10秒)。

The screenshot shows the Cisco FMC Smart Licenses interface. At the top, there is a navigation bar with the Cisco logo and the text 'FMC Smart Licenses'. The main navigation menu includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intellig'. A red error message box is displayed at the top right, stating 'Error The token you have entered is invalid.' Below the error message, there is a 'Welcome to Smart Licenses' section with a 'Register' button. Underneath, there is a 'Smart License Status' table.

Smart License Status	
Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--
Cisco Success Network:	--
Cisco Support Diagnostics:	--

解決策：有効なトークンを使用します。

ケース スタディ 2無効なDNS

症状：次の図に示すように、しばらくしてから（25秒以内）CSSMへの登録が失敗しました。

The screenshot shows the Cisco Firepower Management Center Smart Licenses interface. At the top, there is a navigation bar with the Cisco logo and the text 'Firepower Management Center System / Licenses / Smart Licenses'. The main navigation menu includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. A red error message box is displayed at the top right, stating 'Error Failed to send the message to the server. Please verify the DNS Server/HTTP Proxy settings.' Below the error message, there is a 'Welcome to Smart Licenses' section with a 'Register' button. Underneath, there is a 'Smart License Status' table.

Smart License Status	
Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--
Cisco Success Network:	--
Cisco Support Diagnostics:	--

/var/log/process_stdout.logファイルを確認します。DNSの問題が見られます。

<#root>

```
root@FMC2000-2:/Volume/home/admin#
```

```
cat /var/log/process_stdout.log
```

```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_cur1_send_msg[494], failed to perform, err code 6, err string
```

```
"Couldn't resolve host name"
```

解決策：CSSMホスト名の解決に失敗しました。解決策は、DNSが設定されていない場合はDNSを設定し、DNSの問題を修正することです。

ケース スタディ 3無効な時間値

症状：次の図に示すように、しばらくしてから（25秒以内）CSSMへの登録が失敗しました。

Firepower Management Center
System / Licenses / Smart Licenses

Overview Analysis Policies Devices Objects AMP

Error Failed to send the message to the server. Please verify the DNS Server/HTTP Proxy settings.

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register

Register

Smart License Status

Usage Authorization:	--
Product Registration:	Unregistered
Assigned Virtual Account:	--
Export-Controlled Features:	--
Cisco Success Network:	--
Cisco Support Diagnostics:	--

/var/log/process_stdout.logファイルを確認します。証明書の問題が発生します。

<#root>

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_request_init[59]  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_post_prepare[299]  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_post_prepare[302]  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_cur1_head_init[110],  
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-ERROR: ch_pf_cur1_send_msg[494],
```

```
failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"
```

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_http_unlock[330], unl
```

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_send_http[365], send
```

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_issue[51
```

```
cert issue checking, ret 60, url https://tools.cisco.com/its/service/oddce/services/DDCEService
```

FMCの時刻の値を確認します。

```
<#root>
```

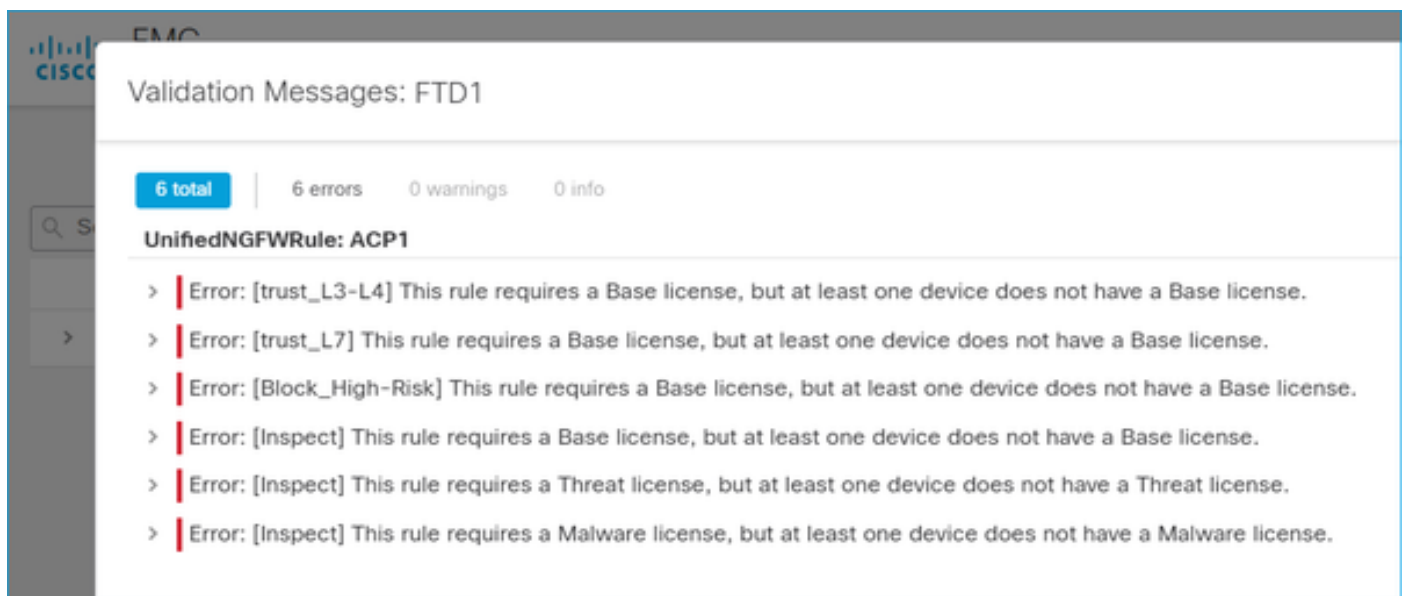
```
root@FMC2000-2:/Volume/home/admin#
```

```
date
```

```
Fri Jun 25 09:27:22 UTC 2021
```

ケース スタディ 4サブスクリプションなし

特定の機能のライセンスサブスクリプションがない場合、FMCの導入は不可能です。



解決策：必要なサブスクリプションを購入してデバイスに適用する必要があります。

ケース スタディ 5コンプライアンス違反(OOC)

FTDサブスクリプションの権限がない場合、FMCスマートライセンスはコンプライアンス違反(OOC)状態になります。

Firepower Management Center
System / Licenses / Smart Licenses

Overview Analysis Policies Devices

Smart License Status

Cisco Smart Software Manager ✖ ↻

Usage Authorization:	✖	Out of Compliance (Last Synchronized On Jun 25 2020)	Re-Authorize
Product Registration:	✔	Registered (Last Renewed On Jun 25 2020)	
Assigned Virtual Account:		KRK-NGFW	
Export-Controlled Features:		Enabled	
Cisco Success Network:		Disabled ℹ	
Cisco Support Diagnostics:		Disabled ℹ	

CSSMで、エラーのアラートを確認します。

General Licenses Product Instances Event Log

Available Actions Manage License Tags License Reservation... 🔒 Search by License 🔍 By Name By Tag

License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> FPR4110 Threat Defense Threat Protection	Prepaid	75	2	+ 73		Actions
<input type="checkbox"/> FPR4110 Threat Defense URL Filtering	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/> FPR4115 Threat Defense Malware Protection	Prepaid	0	1	-1	✖ Insufficient Licenses	Actions
<input type="checkbox"/> FPR4115 Threat Defense Threat Protection	Prepaid	0	1	-1	✖ Insufficient Licenses	Actions
<input type="checkbox"/> FPR4115 Threat Defense URL Filtering	Prepaid	0	1	-1	✖ Insufficient Licenses	Actions
<input type="checkbox"/> FPR4120 Threat Defense Malware Protection	Prepaid	75	0	+ 75		Actions
<input type="checkbox"/> FPR4120 Threat Defense Threat Protection	Prepaid	75	0	+ 75		Actions

ケース スタディ 6強力な暗号化なし

Baseライセンスのみを使用する場合、FTD LINAエンジンでData Encryption Standard(DES)暗号化が有効になります。この場合、より強力なアルゴリズムを使用したL2Lバーチャルプライベートネットワーク(VPN)などの導入は失敗します。

Validation Messages ✕

Device
● FTD1 2 total | 1 error 1 warning 0 info

Site To Site VPN: FTD_VPN

▼ Error: Strong crypto (i.e encryption algorithm greater than DES) for VPN topology FTD_VPN is not supported. This can be because FMC is running in evaluation mode or smart license account is not entitled for strong crypto.
MSG_SEPARATOR IKEv2 PolicyTITLE_SEPARATORAES-GCM-NULL-SHA MSG_SEPARATORMSG_SEPARATOR

Firepower Management Center
System / Licenses / Smart Licenses

Overview Analysis Policies Devices

Smart License Status

Cisco Smart Software Manager ✕ ↻

Usage Authorization:	✓	Authorized (Last Synchronized On Jun 25 2020)
Product Registration:	✓	Registered (Last Renewed On Jun 25 2020)
Assigned Virtual Account:		KRK-NGFW
Export-Controlled Features:	Disabled	Request Export Key
Cisco Success Network:	Enabled	ℹ
Cisco Support Diagnostics:	Disabled	ℹ

解決策：CSSMにFMCを登録し、Strong Encryption属性を有効にします。

追加情報

スマートライセンスの状態の通知の設定

SSMによる電子メール通知

SSM側では、SSM電子メール通知により、さまざまなイベントの要約電子メールを受信できます。たとえば、ライセンスの不足や期限切れ間近のライセンスに関する通知などです。製品インスタンスの接続または更新の失敗の通知を受け取ることができます。

この機能は、ライセンスの期限切れによる機能制限の発生を通知および防止するのに非常に便利です。

Smart Software Licensing

[Alerts](#) | [Inventory](#) | [License Conversion](#) | [Reports](#) | [Email Notification](#) | [Satellites](#) | [Activity](#)

Email Notification

Daily Event Summary

Receive a daily email summary containing the events selected below

Email Address:

Alert Events:

- Insufficient Licenses - Usage in account exceeds available licenses
- Licenses Expiring - Warning that term-limited licenses will be expiring. Sent 90, 60, 30, 14, 7, 3 and 1 day prior to expiration.
- Licenses Expired - Term-limited licenses have expired. Only displayed if Licenses Expiring warning have not been dismissed.
- Product Instance Failed to Connect - Product has not successfully connected during its renewal period
- Product Instance Failed to Renew - Product did not successfully connect within its maximum allowed renewal period.
- Satellite Synchronization Overdue - Satellite has not synchronized within the expected time period.
- Satellite Unregistered and Removed - Satellite failed to synchronize in 90 days and has been removed.
- Licenses Not Converted - One or more traditional licenses were not automatically converted to Smart during Product Instance Registration.

Informational Events:

- New Licenses - An order has been processed and new licenses have been added to the account
- New Product Instance - A new product instance has successfully registered with the account
- Licenses Reserved - A product instance has reserved licenses in the account

Status Notification

Receive an email when a Satellite synchronization file has finished processing by Smart Software Manager

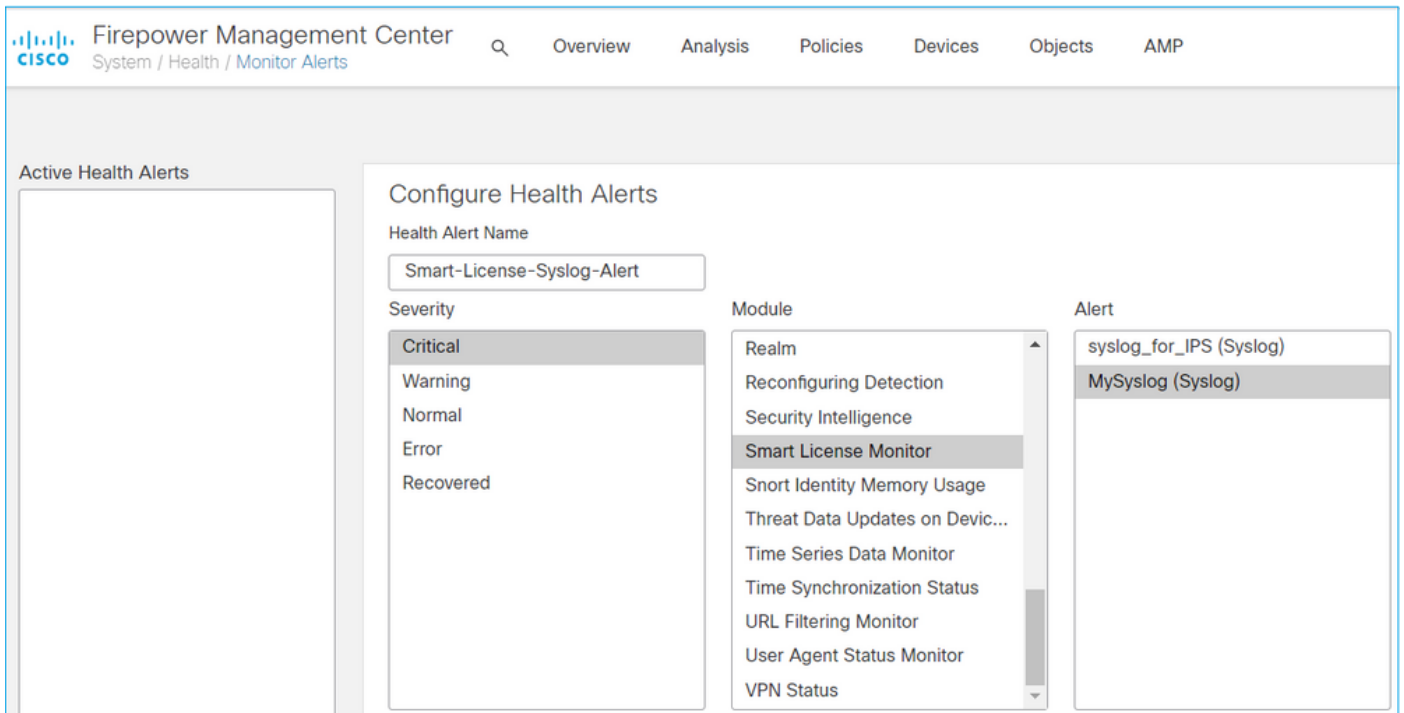
Save

Reset

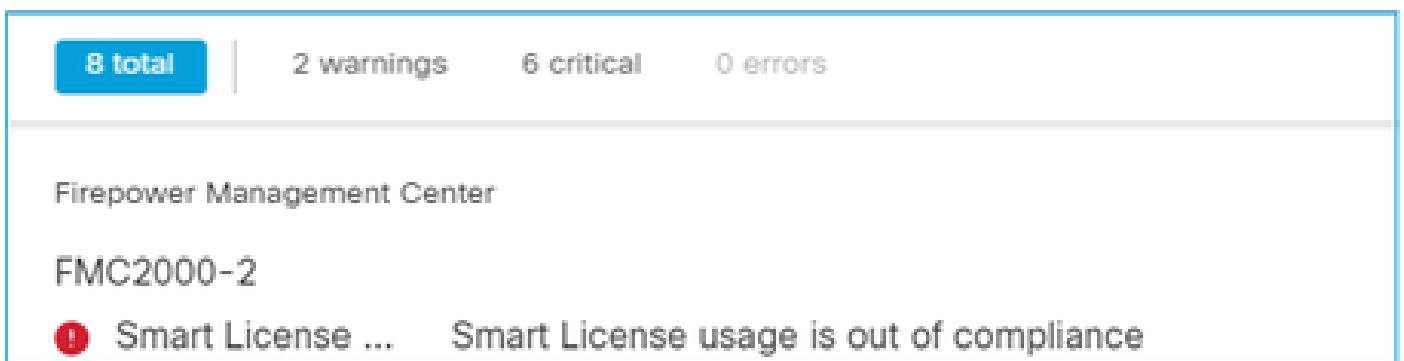
FMCからのヘルスアラート通知の取得

FMC側では、ヘルスマニタアラートを設定し、ヘルスイベントのアラート通知を受信することができます。モジュールスマートライセンスモニタを使用して、スマートライセンスのステータスを確認できます。モニタアラートは、Syslog、電子メール、およびSNMPトラップをサポートします。

スマートライセンスモニタイベントが発生したときにSyslogメッセージを取得する設定例を次に示します。



ヘルスアラートの例を次に示します。



FMCによって生成されるSyslogメッセージは次のとおりです。

```
<#root>
```

```
Mar 13 18:47:10 xx.xx.xx.xx Mar 13 09:47:10 FMC :
```

```
HMNOTIFY: Smart License Monitor (Sensor FMC)
```

```
: Severity: critical: Smart License usage is out of compliance
```

ヘルスマニタアラートの詳細については、『[ヘルスマニタリング](#)』を参照してください。

同じスマートアカウントの複数のFMC

同じスマートアカウントで複数のFMCを使用する場合、各FMCホスト名は一意である必要があります。CSSMで複数のFMCが管理されている場合、各FMCを区別するために、各FMCのホスト名

は一意である必要があります。これは、動作中のFMCスマートライセンスメンテナンスに役立ちます。

FMCがインターネット接続を維持する必要がある

登録後、FMCは30日ごとにスマートライセンスクラウドとライセンスのステータスを確認します。FMCが90日間通信できない場合、ライセンスされた機能は維持されますが、Authorization Expiredステータスのままになります。この状態でも、FMCは引き続きスマートライセンスクラウドへの接続を試みます。

複数のFMCvの導入

仮想環境でFirepowerシステムを使用する場合、クローン（ホットまたはコールド）は正式にはサポートされません。各Firepower管理センター(FMCv)は、内部に認証情報を持つため、一意です。複数のFMCvを導入するには、FMCvをOpen Virtualization Format(OVF)ファイルから一度に1つずつ作成する必要があります。この制限の詳細については、『[Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide](#)』を参照してください。

FAQ

FTD HAでは、必要なデバイスライセンスはいくつですか。

ハイアベイラビリティで2つのFTDを使用する場合は、デバイスごとにライセンスが必要です。たとえば、侵入防御システム(IPS)と高度なマルウェア防御(AMP)機能をFTD HAペアで使用する場合は、2つの脅威およびマルウェアライセンスが必要です。

FTDでAnyConnectライセンスが使用されないのはなぜですか。

FMCをスマートアカウントに登録した後、AnyConnectライセンスが有効になっていることを確認します。ライセンスを有効にするには、FMC > Devicesの順に選択し、デバイスを選択してLicenseを選択します。鉛筆アイコンを選択しますスマートアカウントに保存されているライセンスを選択し、Saveを選択します。

100人のユーザが接続しているにもかかわらず、スマートアカウントで1つのAnyConnectライセンスしか「使用中」ではないのはなぜですか。

スマートアカウントは、このライセンスが有効で、アクティブユーザが接続していないデバイスの数を追跡するため、これは正常な動作です。

エラーが発生した理由 Device does not have the AnyConnect License FMCによるリモートアクセスVPNの設定と導入の後

FMCがスマートライセンスクラウドに登録されていることを確認します。FMCが未登録または評価モードの場合は、リモートアクセス設定を導入できないという正常な動作が発生します。FMCが登録されている場合は、AnyConnectライセンスがスマートアカウントに存在し、デバイスに割り当てられていることを確認します。

ライセンスを割り当てるには、ナビゲート からFMCデバイス、デバイスの選択、ライセンス

(鉛筆アイコン)を参照。スマートアカウントでライセンスを選択し、保存します。を参照。

エラーが発生した理由 Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled リモートアクセスVPN設定の導入が行われるのはいつですか。

FTDに導入されたリモートアクセスVPNでは、Strong Encryptionライセンスを有効にする必要があります。ENfmcで強力な暗号化ライセンスが有効になっていることを確認します。強力な暗号化ライセンスのステータスを確認するには、ナビゲート「FMCシステム>ライセンス>スマートライセンスエクスポート制御された機能が有効になっていることを確認します。

次の場合に強力な暗号化ライセンスを有効にする方法 Export-Controlled Features 無効になっていますか。

この機能は、FMCをスマートアカウントクラウドに登録する際に使用されるトークンで、このトークンが有効になっている製品に対して輸出規制機能を許可するオプションが設定されている場合に、自動的に有効になります。トークンでこのオプションが有効になっていない場合は、FMCの登録を解除し、このオプションを有効にして再登録します。

トークンの生成時に、[このトークンに登録されている製品でエクスポート制御機能を許可する]オプションを使用できない場合はどうすればいいですか。

シスコアカウントチームにお問い合わせください。

「Strong crypto (つまり、VPNトポロジs2の暗号化アルゴリズムがDESより大きい) is not supported」というエラーが表示されるのはなぜですか。

このエラーは、FMCが評価モードを使用している場合、またはスマートライセンスアカウントに強力な暗号化ライセンスが付与されていない場合に表示されます。VFMCがライセンス認証局(RA)に登録されていることを確認し、このトークンに登録されている製品でエクスポート制御機能を許可するが有効になっていることを確認します。スマートアカウントに強力な暗号化ライセンスの使用が許可されていない場合、DESよりも強力な暗号を使用したVPNサイト間設定の展開は許可されません。

FMCで「Out of Compliance」ステータスが受信されるのはなぜですか。

管理対象デバイスの1つが使用不可能なライセンスを使用すると、デバイスがコンプライアンス違反になる可能性があります。

「Out of Compliance」ステータスを修正するにはどうすればよいですか。

『Firepowerコンフィギュレーションガイド』で説明されている手順に従ってください。

1. ページの下部にあるスマートライセンスのセクションを見て、必要なライセンスを判断します。

2.通常のチャネルを通じて必要なライセンスを購入します。

3. Cisco Smart Software Manager(<https://software.cisco.com/#SmartLicensing-Inventory>)仮想アカウントにライセンスが表示されることを確認します。

4. FMCで、System > Licenses > Smart Licensesの順に選択します。

5. Re-Authorizeを選択します。

手順の詳細については、『[Firepowerシステムのライセンス取得](#)』を参照してください。

firepower Threat Defense Baseにはどのような機能がありますか。

Baseライセンスでは次のことが可能です。

- スイッチおよびルーティングするFTDデバイスの設定 (DHCPリレーおよびNATを含む)。
- ハイアベイラビリティ(HA)モードでのFTDデバイスの設定。
- firepower9300シャーシ内のクラスタとしてのセキュリティモジュールの設定 (シャーシ内クラスタ)。
- firepower9300またはFirepower4100シリーズデバイス(FTD)のクラスタとしての設定 (シャーシ間クラスタ)。
- ユーザおよびアプリケーション制御の設定、およびアクセス制御規則へのユーザおよびアプリケーションの条件の追加。

firepower Threat Defense Baseフィーチャライセンスの入手方法を教えてください。

firepower脅威対策またはFirepower脅威対策の仮想デバイスを購入するたびに、Baseライセンスが自動的に含まれます。FTDがFMCに登録されると、スマートアカウントに自動的に追加されません。

FMCとSmart License Cloud間のパスで許可する必要があるIPアドレスはどれか？

FMCはIPアドレス ポート443でスマートライセンスクラウドと通信します。

このIPアドレス(<https://tools.cisco.com>)次のIPアドレスに解決されます。

- 72.163.4.38
- 173.37.145.8

関連情報

- [Firepower Management Centerコンフィギュレーションガイド](#)
- [Cisco Live Smart Licensingの概要 : BRKARC-2034](#)
- [Cisco Secure Firewall Management Center機能ライセンス](#)

- [Cisco Smart Software Licensingに関するFAQ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。